INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
400 ARMY NAVY DRIVE
ARLINGTON, VIRGINIA 22202–4704

May 3, 2007

INSPECTOR GENERAL INSTRUCTION 7950.4

COMPUTER ANTIVIRUS PROGRAM

FOREWORD

This Instruction establishes the Department of Defense Office of Inspector General Computer Antivirus Program. It describes types of malware and related causes, provides procedures for dealing with suspected virus attacks, and defines the responsibilities of the Computer Antivirus Program.

This Instruction is effective immediately.

FOR THE INSPECTOR GENERAL:

for Jonilynn M. Poladeck
Stephen D. Wilson
Assistant Inspector General for
Administration and Management

2 Appendices – a/s

A. Purpose. This Instruction updates the Department of Defense Office of Inspector General (DoD OIG) Computer Antivirus Program. Additionally, it provides procedures for dealing with suspected virus attacks.

B. References. See Appendix A.

C. Cancellation. This Instruction supersedes IGDINST 7950.4, *Microcomputer Antivirus Program*, February 6, 2001.

D. Applicability

1. This Instruction applies to the Offices of Inspector General, the Deputy Inspectors General, the Assistant Inspectors General who report to the Inspector General, the General Counsel, and the Director, Equal Employment Opportunity, hereafter referred to collectively as the OIG Components.

2. This Instruction applies to all OIG computers anywhere in the world, whether or not they are connected to the OIG Local Area Network (LAN), the OIG Wide Area Network (WAN), the Virtual Private Network (VPN), or any other network operated by the OIG.

E. Definitions. See Appendix B.

F. Policy

1. The OIG shall minimize opportunities for the introduction of malware through user protective measures and compliance with DoD and OIG policies.

2. Failure to adhere to this Instruction could result in the discontinuance of user access to the OIG LAN/WAN and/or disciplinary action. Employees who negligently or intentionally misuse computers may be subject to criminal prosecution, civil fines and penalties, and/or agency administrative actions. Depending on the violation, administrative actions could consist of disciplinary action to include removal from Federal service, revocation of a security clearance, or removal from a sensitive position. When such actions are taken, applicable laws, regulations, and procedures will be followed, including, but not limited to, reference (a).

3. Users shall report immediately any violation of this Instruction to their immediate supervisor; the Office of Security, and the Information Systems Directorate (ISD).

G. Responsibilities

1. The **ISD** shall:

   a. Develop instructions for antivirus software use.

   b. Coordinate the OIG Computer Antivirus Program.

c. Designate an antivirus administrator and an alternate antivirus administrator. The antivirus administrator shall install antivirus software on the OIG servers, update antivirus software on a routine basis, administer the installation of antivirus software on user computers, monitor antivirus software use, support the repair or removal of infected files discovered on the OIG computer hardware and software, and perform other antivirus administrative functions.

d. Provide antivirus software updates to all users connected to the LAN at reasonable time intervals.

e. Create and maintain a library of up-to-date malware scanning and eradication software.

f. Return the user to the standard OIG configuration when the ISD determines that hardware or software introduced by the user is causing malfunctions of standard OIG hardware or software, in accordance with reference (b). While every effort shall be made to recover critical data, the ISD shall not assume responsibility for any lack of functionality or any loss of data by returning to the standard OIG configuration.

g. Determine whether to restore network access, in coordination with the Designated Approval Authority (DAA) to users whose password and/or user identification are disabled.

h. Scan commercially purchased software with malware eradication software before use on an OIG computer. When software is purchased in quantity, scan one copy per batch before the software is distributed and loaded on OIG computers. Scanning shall be documented before distribution.

i. Provide written notification to the affected OIG Component Head, the Office of Security, and the Chief Information Officer (CIO) of a malware attack, stating the nature of the malware, effects on hardware or software, damage, possible origin, and corrective action taken to repair any damage.

j. Report incidents to the DoD in accordance with reference (c), as explained in http://www.dtic.mil/doctrine/jel/new_pubs/jp3_13.pdf.

k. Refer apparent violations of this policy for further investigation to appropriate parties.

2. **Users** shall:

a. Operate the hardware or software within established laws, guidelines, and procedures, including software licensing agreements.

b. Minimize the use of bootable floppy diskettes or other bootable media on ISD provided computers.

c. Scan hardware or software used outside the OIG environment before reintroducing it to the OIG environment.

d. Be alert to symptoms that can occur when a computer virus infects a computer, such as continuous rebooting, an unexpected message, or an electronic mail (e-mail) message with suspicious information.

e. Lock the computer by removing their Common Access Card (CAC) or using a software lock (such as pressing CTRL-ALT-DELETE and selecting Lock the Computer), logout of the OIG LAN/WAN, or reboot computers when leaving the computer unattended or upon completion of the work performed. If users are connected to a system maintained outside the OIG, they shall follow supplied log off instructions.

f. Write-protect floppy diskettes unless copying or saving data to the diskette.

g. Protect user identifications and passwords from compromise.

h. Regularly scan hard disks, floppy diskettes, compact disks (CD), digital versatile disk (DVD) and other digital solid state media for malware. Users should ask their Information Systems Liaison Working Group (ISLWG) representatives or the Information Center (IC) for assistance if they are unfamiliar with the process of scanning.

i. Ensure current antivirus software and virus definition files are installed on each applicable computer on a weekly basis. If a computer is physically connected to the OIG LAN with a network cable for at least half an hour, this process is performed automatically. If a laptop or other computing device has not been connected physically for a week or more, the user must reconnect the device to the network and allow enough time for the automatic update to take place. Users connected to the Internet on a non-OIG network may update their virus definitions manually . Users should contact their ISLWG representatives or the IC for assistance if they are unfamiliar with the update process.

j. Regularly back up data by copying data to media other than where the data is currently stored.

k. Not disable antivirus software settings and not remove antivirus software from any government owned computing device unless the ISD instructs the software be removed.

l. Report suspected virus attacks to the ISD in accordance with reference (d) and OIG component-established procedures.

3. The **OIG Component Heads** shall:

a. Devise internal procedures to ensure implementation of the provisions of this Instruction and references (b) through (f), including internal management control mechanisms.

b. Prepare necessary justifications for restoration of user access.

c. Contact the Human Capital Advisory Services (HCAS), for advice and assistance in determining appropriate disciplinary or administrative action. Coordinate disciplinary action, if any, with the HCAS.

4. The **Workforce Relations Division** shall assist and advise the OIG Component Heads on appropriate disciplinary actions if a user violates this Instruction.

5. The **Office of Security** shall conduct a security review, when appropriate.

6. The **Component Information System Security Officer (ISSO)** shall oversee the provisions set forth in this Instruction.

H. Procedures

1. Users shall ensure that their computers are scanned at least once each working day. If the automated scan set by the ISD, is not running as scheduled, the user shall perform this scan. The OIG Component Heads may encourage automatic virus scanning during non-duty hours for more efficient use of computers during the duty day.

2. Users shall ensure that every floppy diskette, CD, DVD and other digital solid state media for is scanned malware.

3. If malware appears at any other time, users shall run antivirus software. If malware is detected on a classified system, the user must report it immediately to the antivirus administrator and the Office of Security, to determine the source and impact of the virus.

4. Users shall request help from the IC if the antivirus software indicates malware is present still or the infected file has been sent to quarantine.

5. The antivirus administrator shall review and attempt to clean up all infected files sent to quarantine. If the antivirus administrator cannot clean up the infected files, he or she shall consult with the manufacturer of the antivirus software or other sources for help.

6. Users shall follow any instructions about malware attacks in e-mail messages within one hour of reading the e-mail message.

7. Users shall report suspected malware attacks to the IC in accordance with reference (d). The OIG Component Heads shall determine internal reporting procedures.

8. If malware affects more than one computer or if malware affects a network server the ISD shall prepare and oversee execution of a virus eradication plan.

9. Users located at 400 Army Navy Drive or those connected by frame relay to the LAN/WAN shall update virus definitions as described in paragraph G.2.i. Other users should contact the ISD to arrange antivirus definition updates.

APPENDIX A
REFERENCES

a. IGDINST 1400.4, *Disciplinary and Adverse Action*, June 5, 2006

b. IGDINST 7950.2, C*omputer Hardware and Software Management Program*, May 3, 2007

c. Chairman Joint Chiefs of Staff Notice 3-13 *Information Operations*, February 13, 2006
http://www.dtic.mil/doctrine/jel/new_pubs/jp3_13.pdf

d. IGDINST 7920.51, *Resolving User Problems*, May 3, 2007

e. IGDINST 5200.40, *Security Requirements for Automated Information Systems (AIS)*, July 20, 2000

f. IGDINST 7920.5, *Small Computer Use*, May 3, 2007

APPENDIX B
DEFINITIONS

1. **Bootable** means that a diskette, Zip disk, compact disk (CD), or other type of media holds a set of instructions that can start or restart a computer system by reading initialization instructions into the computer's memory.

2. **Bootleg Software** refers to the illegal duplication and distribution of software and software documentation. Bootleg takes two specific forms--counterfeit and pirate.

a. Counterfeit Software. The unauthorized simulation of prewritten programs, as well as the unauthorized duplication of original artwork, labels, trademarks, and packaging of prewritten programs produced by obtaining a legitimate copy of the software and simulating the functions.

b. Pirate Software. The unauthorized duplication of legitimate copies of programs produced by procuring legitimate copies of software and duplicating them without having a license to make the copies.

3. **Chief Information Officer (CIO)** is the senior official appointed by the IG who is responsible for developing and implementing information resources management in ways that enhance the OIG mission performance through the effective, economic acquisition and use of information. The CIO is the Assistant Inspector General for Administration and Management.

4. **Computer** is a device that has self-contained processing units and are transportable easily. The definition includes, but is not limited to, equipment that may be referred to as palmtop computers, hand held computers, personal digital assistant computers, personal computers, desktop computers, laptop computers, and notebook computers.

5. **Environment** includes the mode of operation of an information system, the hardware, the software, the internal operating system, and any external operating systems. Those operating systems include, but are not limited to, DOS, Windows, UNIX, Intranet, and Internet.

6. **Hardware** is equipment supporting an automated information system. An information system is the organized collection, processing, transmission, and dissemination of information according to defined procedures.

7. **Information** is any communication or reception of knowledge, such as facts, data, or opinions, including numerical, graphic, or narrative forms, maintained in any medium, including but not limited to, computerized databases, paper, microform, or magnetic tape.

8. **Malware** is any hardware and/or software that modifies a computer system or records, saves and/or transmits user information without the knowledge or consent of the user. Malware consists of, but is not limited to, viruses, worms, trojans, adware, spyware, and key loggers.

DEFINITIONS

9. **Program** is a series of instructions that shall cause a computer to perform tasks.

10. **Software** is a program that tells a computer what to do.

11. **System** is a collection of people, equipment, policies, and methods organized to accomplish an activity.

12. **Virus** as used in this Instruction, includes all malicious software, such as:

a. Bombs. Programs with a trigger for perpetration of a malicious act when particular states of the system are realized.

b. Trap Doors. Hidden commands or entry points into a program module that can be triggered to permit circumvention of system protection mechanisms.

c. Trojan Horses. Programs with a documented legitimate function (actual or apparent) that additionally performs some hidden unauthorized action(s).

d. Worms. Programs that can replicate themselves without becoming an attachment to any other software.

e. True Virus. Defined as malicious code, has the ability to locate other software and make copies of other software and embed itself within the software.

13. **User** is a person with authorized access to OIG computers, information systems, and/or information technology resources

14. **Write-Protect** means to use some type of physical mechanism that prevents modification or erasure of data on a device.